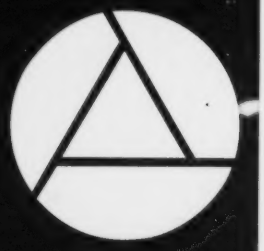
2009/2010 : Report 7



OFFICE OF THE

Auditor General of British Columbia

The PARIS System for Community Care Services:

Access and Security

February 2010

2009/2010 : Report 7

OFFICE OF THE
Auditor General
of British Columbia

The PARIS System for Community Care Services:

Access and Security

February 2010

Library and Archives Canada Cataloguing in Publication Data

British Columbia. Office of the Auditor General.

The PARIS system for community care services : access and security / Office of the Auditor General of British Columbia

(Report ; 2009/2010: 7)

Includes bibliographical references and index.

ISBN 978-0-7726-6243-9

1. Medical records--Access control--British Columbia. 2. Information storage and retrieval systems--Medical care--British Columbia. 3. Health services administration--British Columbia. 4. PARIS (B.C. : Information retrieval system). I. Title. II. Series: British Columbia. Office of the Auditor General. Report ; 2009/2010 : 7.

RA976.B74 2010 353.6'238709711 C2010-900488-4

OFFICE OF THE
Auditor General
of British Columbia

LOCATION:
8 Bastion Square
Victoria, British Columbia
V8V 1X4

OFFICE HOURS:
Monday to Friday
8:30 a.m. – 4:30 p.m.

TELEPHONE:
250 387-6803
Toll free through Enquiry BC at: 1 800 663-7867
In Vancouver dial: 604 660-2421

FAX: 250 387-1230

E-MAIL: bcauditor@bcauditor.com

WEBSITE:
This report and others are available at our website, which also contains further information about the Office: www.bcauditor.com

REPRODUCING:
Information presented here is the intellectual property of the Auditor General of British Columbia and is copyright protected in right of the Crown. We invite readers to reproduce any material, asking only that they credit our Office with authorship when any information, results or recommendations are used.

OFFICE OF THE
Auditor General
of British Columbia

8 Bastion Square
Victoria, British Columbia
Canada V8V 1X4
Telephone: 250 387-6803
Facsimile: 250 387-1230
Website: www.bcauditor.com

The Honourable Bill Barisoff
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Sir:

I have the honour to transmit herewith to the Legislative Assembly of British Columbia my 2009/2010 Report 7: The PARIS System for Community Care Services: Access and Security.

John Doyle, MBA, CA
Auditor General of British Columbia

Victoria, British Columbia
February 2010

copy: Mr. E. George MacMinn, Q.C.
Clerk of the Legislative Assembly

Table of Contents

Auditor General's Comments 1

Executive Summary

- Overall Conclusion 5
- Key Findings and Recommendations 6

Response from VCHA 11

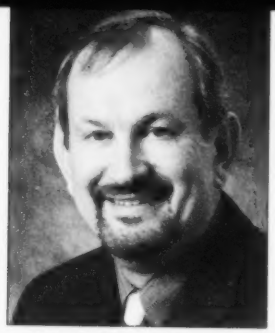
Detailed Report

- Background 15
- What we looked at 17
- What we found 19

Appendix

- A Glossary 29

Auditor General's Comments



John Doyle
Auditor General

Every British Columbian has the right to receive health care in any health care facility in the province. British Columbians expect that their personal information will be managed responsibly and accessed only by those who need it in order to provide care.

Maintaining the confidentiality and integrity of individuals' health care records is profoundly important. Failure by health care organizations to properly manage and safeguard this information could have serious consequences, from compromising an individual's privacy to enabling identity theft or other fraudulent use of personal information to occur.

I undertook an assessment of a clinical information system used by the Vancouver Coastal Health Authority (VCHA) that provides community health care services to more than 620,000 residents of the region. The goal was to assess the security measures used to protect the health care records and information accessible on a specific information system called Primary Access Regional Information System (PARIS).

In every key area we examined—from the management and assignment of user access to security controls within the health authority's computing environment—we found serious weaknesses.

Because PARIS users are not granted access on a "need-to-know" basis, sensitive and confidential health care records were accessible to thousands of users who have neither the need nor the right to see the information. Security controls throughout the network and over the database were so inadequate that there was a high risk of external and internal attackers being able to access or extract information, without VCHA even being aware of it. Fundamental controls to prevent or detect unauthorized access to the system were lacking, and monitoring to determine what data exchanges occurred was also insufficient.

In several areas, the governance and direction that staff needed to build a secure environment were not in place. Staff were not provided guidance on security controls to mitigate risks. The organization did not have an IT security policy and basic security practices (such as building layers of defense within the system) were inadequate.

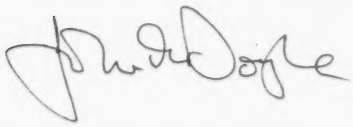
Auditor General's Comments

Due to the seriousness of the deficiencies, I delayed the publication of this audit report to allow sufficient time for VCHA to address the security vulnerabilities we identified, thereby ensuring that this report would not further expose the system to potential compromise.

I have been satisfied with the responsiveness and significant effort that VCHA has put into addressing the most significant problems, in a relatively short time. Over the next months, my staff will continue monitoring the actions of the VCHA in addressing the remaining audit findings.

Based on the conclusions of this audit and other work performed by my staff, some of the fundamental security weaknesses identified in this information system may be present to some degree in other government systems. The findings and recommendations reported here should therefore be of use to other organizations in the health industry, as well as in other sectors. Adequate security controls should be built into any system, and it is equally important to undertake regular reviews of critical systems to ensure that they remain sufficiently secure.

I would like to thank the Vancouver Coastal Health Authority staff for the cooperation and assistance they provided to my staff during this audit.



John Doyle, MBA, CA
Auditor General of British Columbia

Victoria, British Columbia
February 2010

Audit Team

Bill Gilhooly, Assistant Auditor General
Pam Hamilton, IT Audit Specialist
Ada Chiang, IT Audit Specialist
Adel Elassal, IT Consultant

Executive Summary

Executive Summary

Vast amounts of health care information are processed and stored in computer systems, providing instant access to important information and the potential for improving health care delivery. While there is increased availability to information, there is also a public expectation that organizations will be diligent in securing health care information.

PARIS (Primary Access Regional Information System) is a community based health care system used by Vancouver Coastal Health Authority. Information for many services provided to clients is recorded in PARIS—from home and residential care, mental health services and addictions services to infant and youth services and health promotion services. Implementation of the system began in 2002. It is now in more than 75 community locations throughout Vancouver and Richmond. The system links health care information throughout the region to create integrated electronic health care records.

While many benefits can be achieved by the availability of this sensitive information, appropriate measures must be taken in order to secure and protect it. Managing appropriate access to this information can also be particularly challenging in the health care environment, where the primary focus is often on client service delivery.

If adequate controls are not in place, the results could be loss of individual privacy, corruption or manipulation of client information, medical identity theft, or system failure. In our audit, we assessed the level of access granted to PARIS users in the Vancouver Coastal Health Authority (VCHA), and the adequacy of security controls in place to protect the information and the system.

Overall Conclusion

In our examination of access and security, we found significant deficiencies in all the areas we audited of VCHA's computerized health care system (PARIS).

- Almost all system users have excessive access to sensitive and confidential client information. Many clients' full health information is accessible to a large number of users.
- Essential security controls are not in place to detect and prevent unauthorized access or attacks.
- There is a risk that inappropriate disclosure or theft of information could take place without VCHA's knowledge.

Key Findings and Recommendations

We assessed the security controls and procedures in place to protect health information contained in PARIS, and communicated our audit findings to VCHA throughout the audit. In August 2009 we also provided VCHA with a detailed management report that documented our findings and presented 127 recommendations, which were accepted.

VCHA management responded positively when we brought these control weaknesses to their attention, and developed an action plan to address the most significant problems in a relatively short time. They have told us that the most significant deficiencies identified have been fixed. We will continue monitoring progress on their action plan.

We have not published all the details of the findings and recommendations from the detailed management report, to avoid introducing additional security risks. We consolidated the most significant recommendations from the detailed management report into 10 key recommendations. For presentation purposes, we have organized the recommendations into six main audit areas: security policies, system security, database and operating system, application access, account management, and monitoring.

The number of detailed recommendations we made in each of these areas is shown below.

Key audit area	Number of recommendations
Security policies	7
System security	27
Database and operating system	27
Application access	24
Account management	30
Monitoring	12
Total recommendations	**127**

Access is beyond "need-to-know"

Access granted to PARIS client records is excessive, with users in many cases having full, unmonitored access to all client records. The access model is based on a team approach but does not control

access on a "need-to-know" basis. Access to the team-based information is also provided through application menus, which have not been granted consistently according to users' professions.

We recommend that user access to client records be granted based on the principle of "need-to-know." Doing so will require assessing users' job functions, business workflows, team memberships, profession coding, menu structures, and security levels applied to client records.

System security is inadequate

Controls to detect and prevent external or internal attacks are not adequate. The security strategy in place is not built based on a "defence-in-depth" approach to guard against the failure of single security components, software flaws or configuration mistakes.

We recommend that multiple layers of security be implemented. In particular:

- ***firewall and router controls should be strengthened;***
- ***standards to secure all systems should be developed;***
- ***additional firewall layers should be employed;***
- ***intrusion detection systems and intrusion prevention systems should be positioned properly;***
- ***timely and mandatory system patching should be carried out; and***
- ***regular vulnerability testing should be performed.***

Security policies are lacking

The lack of a comprehensive security policy for PARIS has contributed to the absence of other fundamental security controls in the system and of the processes affecting the network, database, operating system and application security. The overall organizational security culture has not set the right tone for a secure environment.

We recommend that comprehensive, up-to-date security policies, approved by senior management, be developed, implemented, and enforced.

Executive Summary

The database is not secure

Lack of proper database security controls means that errant data could be input, data could be corrupted, unauthorized viewing or data extraction could occur. There have been several irregularities, including connections made to the production database by non-production servers; vendors having continuous database access; users gaining access to the database directly through unprotected roles; and support staff having access to powerful database privileges that should be restricted to database administrators.

We recommend that the database be secured by:

- ***restricting database privileges on a "need-to-know" basis;***
- ***removing continual access from vendors;***
- ***securing roles; and***
- ***ensuring that direct access to the database is available only to authorized users through a secure channel.***

Risk of data leakage

There are insufficient controls to ensure that client information stored on PARIS has been safeguarded from inappropriate disclosure for the personal or financial gain of insiders or external intruders. Logs are not monitored; traffic to the database is not restricted; information extracted from the database is not tracked; default passwords have not been changed; and the database management privileges are not properly restricted.

We recommend that controls be implemented to reduce the risk of data leakage. Such controls include:

- ***content monitoring;***
- ***audit trail monitoring;***
- ***properly isolating and firewalling database servers; and***
- ***appropriate access to privileges.***

Executive Summary

Monitoring is inadequate

Inadequate visibility, logging, monitoring, analysis and management of audit trails could result in external or internal attacks going undetected. Most logs are not monitored, limited information is collected, and log management capabilities are insufficient for consolidating and analyzing the logs.

We recommend that logs be:

- ***monitored regularly and all pertinent information collected from them;***
- ***managed to allow for proper analysis;***
- ***secured from tampering; and***
- ***positioned properly to ensure they are effective in preventing and detecting attacks, troubleshooting and tracing activity.***

Access is not properly maintained

Inadequate user ID and password management practices could put the system at risk of unauthorized and undetected access. Processes are not always followed to alert IT administration staff promptly of changes in users' employment status for which account changes must be made. Privileged account passwords are not always changed immediately when users with knowledge of the passwords are no longer employed by the health authority.

We recommend that:

- ***application, network, operating system and remote access accounts be properly managed to ensure that only authorized users have access; and***
- ***processes be followed to ensure access is removed promptly when users no longer require access because of employment status changes.***

Unsecure network access

Current system settings and practices do not restrict unsecure connections to be made into sensitive systems. Physical connections in meeting rooms allow non-VCHA computers to connect to the internal network and the Internet. Unaccounted-for laptops are able to connect to the internal network, remote access servers are allowing connections to bypass perimeter defences, and Virtual

Private Network (VPN) users are granted too much access within the internal network.

We recommend that access methods that could potentially allow unauthorized entry into the network be removed or secured. In particular:

- ***remote access servers allowing dial-in access should be disconnected;***
- ***network access should be disabled for all unaccounted-for laptops;***
- ***network access points in common areas should be better controlled; and***
- ***VPN access should be properly restricted.***

Inadequate traffic control on the internal network

Within the internal network, there are no access control mechanisms to restrict traffic to critical servers or to reduce the spread of viruses or malicious code throughout the network. Devices on the internal network are not positioned to allow for filtering or proper control over the type of traffic permitted to reach them.

We recommend that:

- ***servers be positioned in different network segments with proper traffic filtering; and***
- ***access control restrictions be implemented to permit only legitimate traffic to reach critical servers.***

Record management practices are lacking

No classification system or retention policies are in place to effectively guide or manage the removal or archiving of client records that are no longer relevant. These records therefore remain accessible and viewable in the system indefinitely.

We recommend that an appropriate record classification, retention and disposal scheme be developed, approved and implemented to identify and subsequently remove or archive records on a regular basis.

Response from VCHA

On behalf of the Board and management of Vancouver Coastal Health (VCH), thank you for the opportunity to respond to the comments in the audit report of our community patient information system, PARIS.

As a leader in patient care and innovation, VCH has demonstrated a commitment to explore new technologies to better support quality and safe care for our patients, clients and residents. We know that better access to information enhances care and improves the health care system. We also know that safeguarding that information is crucial—not just to comply with legislation, but to build confidence and trust in those we serve.

Before the implementation of PARIS in the VCH community system in 2001, we had around 40 disparate, independent systems supporting our clinical programs. These systems lacked consistent data and process standards. This lack of cohesive information placed care at risk. PARIS was identified as the solution to this safety concern. PARIS was developed based on protocols at that time by inter-disciplinary teams. PARIS enables care providers to quickly access the important information necessary to address patient/client care needs. Its success has been dependant on expert clinical advice. VCH believes that PARIS has served our community patients and clients well without any demonstrated risk to safety.

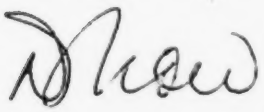
PARIS has strict security protocols that not only protect confidentiality, but comply with established practices and expectations. A recent external security assessment confirmed that VCH's electronic security perimeter was among the top 25% of companies in Canada—even higher when compared to other health care organizations.

As you are aware, VCH has always placed a strong emphasis on the protection and confidentiality of patient/client information. That is why we take reports such as yours extremely seriously. Your audit made a number of recommendations. As you also know, VCH has implemented almost 75% of them already and completed 100% of those in the "high risk" category. Naturally, no recommendation would be implemented that might negatively impact patient care and without confirmation by clinical experts. The level of accessibility to information within PARIS is based on the need to know so as to ensure safe, timely and appropriate care. Information in PARIS is secure and the care, safety and well being of our patients and clients are better because of it.

Response from VCHA

VCH acknowledges it cannot become complacent in the areas of security, confidentiality and protection of privacy. Such procedures and controls have to be refreshed and VCH undertakes a regularly scheduled Security Management Review to ensure they meet current legal obligations, including the requirement of reasonable security precautions. These standards must change in response to innovations in technology and developing practices. VCH is committed to doing this and to being at the forefront of such changes. We have demonstrated that commitment through the speed and vigor at which we responded to your initial recommendations as well as our ongoing security audit processes.

Like you, VCH wants the best for all British Columbians. Your support for improving the health and well being of our communities is appreciated.



Dr. David Ostrow
President and Chief Executive Officer

Detailed Report

Background

Information security and privacy

Technology has significantly enhanced the way health care services are delivered. Electronic information systems assist in the management and delivery of services by providing health care workers with instant access to information about their patients. To enable this, considerable amounts of personal and health information about individual patients are collected and stored in databases.

While the benefits to be gained in using technology for delivering health care are well recognized, preventing unauthorized access to sensitive information is increasingly challenging. Accessing, sharing, copying and transferring information inside or outside the organization must be strictly controlled. If sensitive information were to fall into the wrong hands, not only would public trust in health care systems be seriously threatened but individuals' right to privacy could be lost or identities stolen for fraudulent use.

In the business of delivering public health care, the expectation is that while the personal health information of an individual will be shared with other care providers, the individual's privacy rights will be safeguarded and the information kept secure from unauthorized disclosure.

It is reasonable for British Columbians to expect that the health care information about them is protected and access to it is allowed only when it is needed for providing care. System access should therefore be properly configured, granted, maintained and monitored to ensure information is safeguarded at all times.

The business and computing environment

PARIS (Primary Access Regional Information System) is an information system that collects and reports clinical and administrative information for the Vancouver Coastal Health Authority's community programs.

The system was implemented in phases beginning in 2002, with objectives to:

- improve client care;
- improve the coordination of services amongst community health service providers;
- increase clinical effectiveness by improving access to relevant client information; and
- provide tools to measure client care outcomes.

By having such an integrated electronic clinical system, VCHA believes it has realized benefits in improving the quality of client care, and allowed service areas to more efficiently share patient information.

It is used by many health care providers—community health nurses, health care workers, occupational therapists, physicians, social workers and others—as well as administrative staff to deliver a range of care services to clients across community programs, including:

- primary care – for adult and children;
- home- and community-based residential health care for adult and children;
- mental health services;
- addictions services;
- preventative health;
- rehabilitative care; and
- palliative care.

The PARIS system, which integrates a range of health care workflow processes needed to support care across 76 community locations, forms a central repository of health and administrative information for more than 620,000 clients.

There are different modules in the system with various functions that help to coordinate and integrate care and to enhance operational workflow. These functions include:

- registering a client for health consultation or treatment;
- recording entries about a client's health care status such as illnesses, medication allergies, clinical assessments, planned interventions, and care planning;
- administering preventative health screening events such as immunizations, dental and hearing; and
- managing waitlists for housing placement to support independent living.

Approximately 4,000 people use the system, mostly working at clinics across the region. The PARIS system connects both local and remote users through a complex network. The system's security architecture accommodates a team-based access approach, as well as a more granular one depending on users' association with client.

What we looked at

Audit Purpose and Scope

Our main objective with this examination was to assess the management of access and adequacy of controls in place to protect the client information in the PARIS system used by the Vancouver Coastal Health Authority.

Many components are involved in ensuring the system's security, from access management to numerous technical aspects of the computer networks.

Any computing environment has risks that must be constantly addressed and managed. This report focuses on the key components and the controls relevant to mitigating those risks associated with providing a secure environment for processing health information.

Exhibit 1 shows all the components we included in our audit scope. We did not look at access security of the wireless computing network. Nor did we assess any aspects of patient health care service delivery at VCHA, or the benefits of implementing PARIS.

Exhibit 1:

Components pertaining to security access, covered in the PARIS audit

Source: Compiled by the Office of the Auditor General

In our examination we sought to answer the following questions:

- Are there security policies in place to establish an effective security program?
- Is the network properly secured to protect against internal and external attacks?
- Is access to the database and system properly controlled and secured to guard against unauthorized access and data leakage?
- Is access to health care information restricted based on "need-to-know"?
- Are users authorized and accounts adequately maintained to prevent inappropriate access to sensitive information?
- Is the logging and monitoring of system activity adequate to detect unauthorized access?

Audit Criteria

International standards on which the audit criteria were based are from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC):

- ISO/IEC 27001 on Information Technology - Security Techniques - Information Security Management Systems - Requirements
- ISO/IEC 27002 on Information Technology - Security Techniques - Code of Practice for Information Security Management.

Our audit criteria were based on international standards issued by the International Organization for Standardization and the International Electrotechnical Commission (see sidebar)[1]. These guidelines provided standard control objectives against which we assessed the design and effectiveness of VCHA's information technology controls.

We conducted the audit in accordance with the assurance standards recommended by the Canadian Institute of Chartered Accountants, and accordingly included tests and other procedures we considered necessary to obtain sufficient and appropriate evidence to support our conclusions.

We carried out the audit during the period October 2008 to May 2009.

What we found

Security policies

Security policies are written directives from senior management based on assessments of potential threats and vulnerabilities to IT systems and data. They should lay out an overall security program and give direction to all levels of staff as to the controls and procedures that should be in place to mitigate identified risks. Equally important, they should set the tone for security throughout the organization.

[1] The ISO standards have been used as the framework for setting the security requirements for an interoperable electronic health record (EHR) by the Canadian Health Infoway (CHI) Inc. CHI is a not-for-profit organization funded by the federal government that works with the provinces and territories to accelerate the development and use of interoperable electronic health information systems across Canada. We have considered the CHI security requirements in the development of our audit criteria.

Key Findings

We found that a comprehensive security policy for PARIS does not exist.

- Only a few security policies are in place, and some of those have only recently been established.
- In all of the IT areas we assessed, we found little guidance provided to IT support staff to tell them what security controls should be implemented.

We made seven detailed recommendations in this area to improve security policies pertaining to PARIS.

System security

Computer networks can enable users to access resources—including the Intranet, applications and databases—from local and remote locations. A common approach for security in network designs is to build in multiple layers of protection to guard against failure of single security components, software flaws, or configuration mistakes.

Key Findings

We found a lack of fundamental security controls in the system to prevent and detect external or internal network attacks.

- There is a gap with respect to firewalling systems that are positioned on the internal network.
- No intrusion prevention and detection systems exist to prevent or detect certain types of attacks.
- The existing processes are not adequate to ensure all perimeter firewall and router rules are authorized and current.
- Vulnerability scans are not run on systems before they are put into production and subsequently while in production.
- Penetration testing is not performed.
- Personal firewalls to protect individual computers from unauthorized network traffic access are not used on all computers.

We also found multiple network attack points, including:

- un-patched servers and devices;
- unnecessary and unsecured services running on servers;
- open network connections in common business areas;
- dial-in remote access servers that bypass perimeter firewall security;
- active network accounts belonging to former employees; and
- unaccounted-for laptops having network connectivity.

We made 27 detailed recommendations in this area to improve system security in PARIS.

Database and operating system

Databases provide structures to hold system and client information. Operating systems host databases and provide interfaces to hardware. Specific controls in both the database and the operating system should be properly implemented to protect the integrity of the information and prevent inappropriate access or unauthorized extraction of information.

Key Findings

We found that controls have not been implemented to provide an adequate level of security over the database and operating system in order to protect the information from being corrupted or inappropriately accessed or extracted.

- Users of PARIS can bypass application controls and enter the database directly through non-password-protected database roles (see glossary). Although the majority would not know this capability existed, awareness of it could allow users the ability to access or extract sensitive client information.
- Application administrators have access to the most powerful database commands—intended only for database administrators. This puts performance and integrity of the database at high risk.
- We found evidence that many connections have been made from non-production servers to the production database environment meaning that incorrect data may have been entered, data may have been corrupted, or unauthorized viewing of data may have occurred.

We also found a lack of fundamental controls in and around the database to ensure that information is protected from inappropriate disclosure for either the personal or financial gain of insiders or external intruders.

- The audit trail is not monitored to identify inappropriate and unauthorized entry.
- No content monitoring tools are used to ensure that only valid data exchanges occur.
- No firewalls are in place to prevent unauthorized access to reach the database server.
- Default passwords have not been changed on well-known accounts, thus giving a potential attacker access to an active database account.
- Unprotected database roles exist, opening up the risk of access by unauthorized users to client data via direct logins to the database.
- Both IT and application support staff have full, unmonitored access to all information.
- Open vendor accounts exist, allowing health care data to be copied even outside the Vancouver Coastal Health Authority at any time.

We made 27 detailed recommendations in this area to improve the management and security of PARIS's database and operating system.

Application access

Managing access to client records in the health care industry is challenging. Too much access means that clients' privacy rights could be violated. Not enough access means that clients' safety could be at risk. Finding the right balance is essential. To ensure that accesses are granted and maintained in accordance with approved management decisions, security models should be established, documenting the access; and well-designed processes should be in place to ensure that accesses remain current and appropriate.

Key Findings

We found that the access granted to health care workers and other application users of PARIS well exceeded what was needed or reasonable.

- User access is not managed on a "need-to-know" basis.
- Almost all users have some access to confidential information about all clients in the database.
- Many clients' full health information is accessible to a large number of users.
- The auditing procedures currently in place are not capable of detecting inappropriate access by users to client information.
- No archiving or deletion strategy is in place, which means that former client records and irrelevant records for current clients are still accessible to system users.

We also found that the controls and processes in place are not adequate to ensure that accesses to PARIS are correct and up-to-date.

- No security matrices have been established to show what access users should have, based on their job functions.
- Management-approved decisions are not maintained to support the access granted to users at a role-based or team-based level.
- Team memberships are not up-to-date, meaning that many unauthorized users could have access to client records they should not have.
- Profession coding is not consistently applied, which could result in improper granting of role-based access.
- The access given to users through the application menu has not been granted on a "need-to-know basis", which again means that unauthorized users could view client records.

We made 24 detailed recommendations in this area to improve user access through the PARIS application.

Account management

Account management is a process that defines who can access particular applications, databases, as well as all other resources and services available on a network. Users are given approval to access these resources while they maintain a certain relationship with the organization, usually through employment or a contract. When the relationship ends, the access should also immediately end.

Staffing movements within an organization are normal and in many cases will necessitate changes in access rights. Well-established procedures should therefore be in place for making adjustments to remove or change user access as needed.

Key Findings

We found that some users with former employment or contractual relationships with the Vancouver Coastal Health Authority are still able to access the PARIS network and its resources.

- Processes are not always followed to remove or change a user's access when his or her employment or contractual status changes.
- We found that hundreds of former users, both employees and contractors, still have access to resources through active application accounts, network accounts and Virtual Private Network accounts.
- Passwords for powerful, privileged IT support accounts have, in some cases, not been changed even though users who know the passwords have left the employment of the health authority.

We made 30 detailed recommendations in this area to improve account management in PARIS.

Monitoring

Proper visibility into systems is critical for detecting internal and external attacks. Log management capabilities, including consolidation, collection of all pertinent information and adequate analysis tools should be in place to allow for effective monitoring.

Key Findings

We found inadequate processes in place for detecting attacks.

- Most logs (including the database audit trail) are not monitored.
- No log management capabilities exist to consolidate logs and allow for effective analysis.
- Pertinent information is not collected, so it is not possible to determine whether unauthorized access to systems has ever occurred.
- The logs are not properly secured to protect against tampering or deletion.

We made 12 detailed recommendations in this area to improve monitoring of PARIS.

Appendix

Appendix A: Glossary

Database

A database is a collection of information organized in such a way that a computer program can quickly select desired pieces of data. You can think of a database as an electronic filing system. (*Source: www.webopedia.com*)

Database roles

Database roles allow access to be indirectly assigned to users. By using roles, users do not have to be given direct access to data. Tables, views, procedures and other database objects are assigned to roles and roles are assigned to users. Roles are generally assigned many more tables than each user needs, but through the application controls the users will be limited to only the information they are authorized to access.

Encryption

Encryption is the translation of data into a secret code and is an effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. (*Source: www.webopedia.com*)

Firewall

A firewall is designed to prevent unauthorized access to or from a network. It can be hardware, software, or a combination of both. All messages entering or leaving the network through the firewall are examined and those that do not meet the specified security criteria are blocked. (*Source: www.webopedia.com*)

Intrusion detection system

An intrusion detection system (IDS) inspects and alerts on inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system and its resources. (*Source: www.webopedia.com*)

Intrusion prevention system

An intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. (*Source: www.wikipedia.org*)

Operating system

An operating system is the program that manages all other programs in the computer. Other programs make use of the operating system by making requests for services. Users can also interact directly with the operating system.

Patch

A patch is a code supplied by the software vendor and inserted into the executable program. Patches are used to fix bugs and security vulnerabilities, and to introduce new program features.

Appendix A: Glossary

Penetration test

A penetration test is a method of evaluating the security of a computer system or network by simulating an attack. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. (*Source: www.wikipedia.org*)

Personal firewall

A personal firewall is software installed on an individual computer. It protects only the computer it is installed on. Based on security policies set within the firewall, network traffic can be permitted or denied.

Router

A router is a device that forwards data packets along networks. Routers are located at gateways where two or more networks connect. (*Source: www.webopedia.com*)

Virtual Private Network (VPN)

A VPN, or virtual private network, is a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted or altered. (*Source: www.webopedia.com*)

Vulnerability scanning

Vulnerability scanning is the automated process of proactively identifying vulnerabilities of computing systems in a network to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they also open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known ones, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten network security. (*Source: www.webopedia.com*)